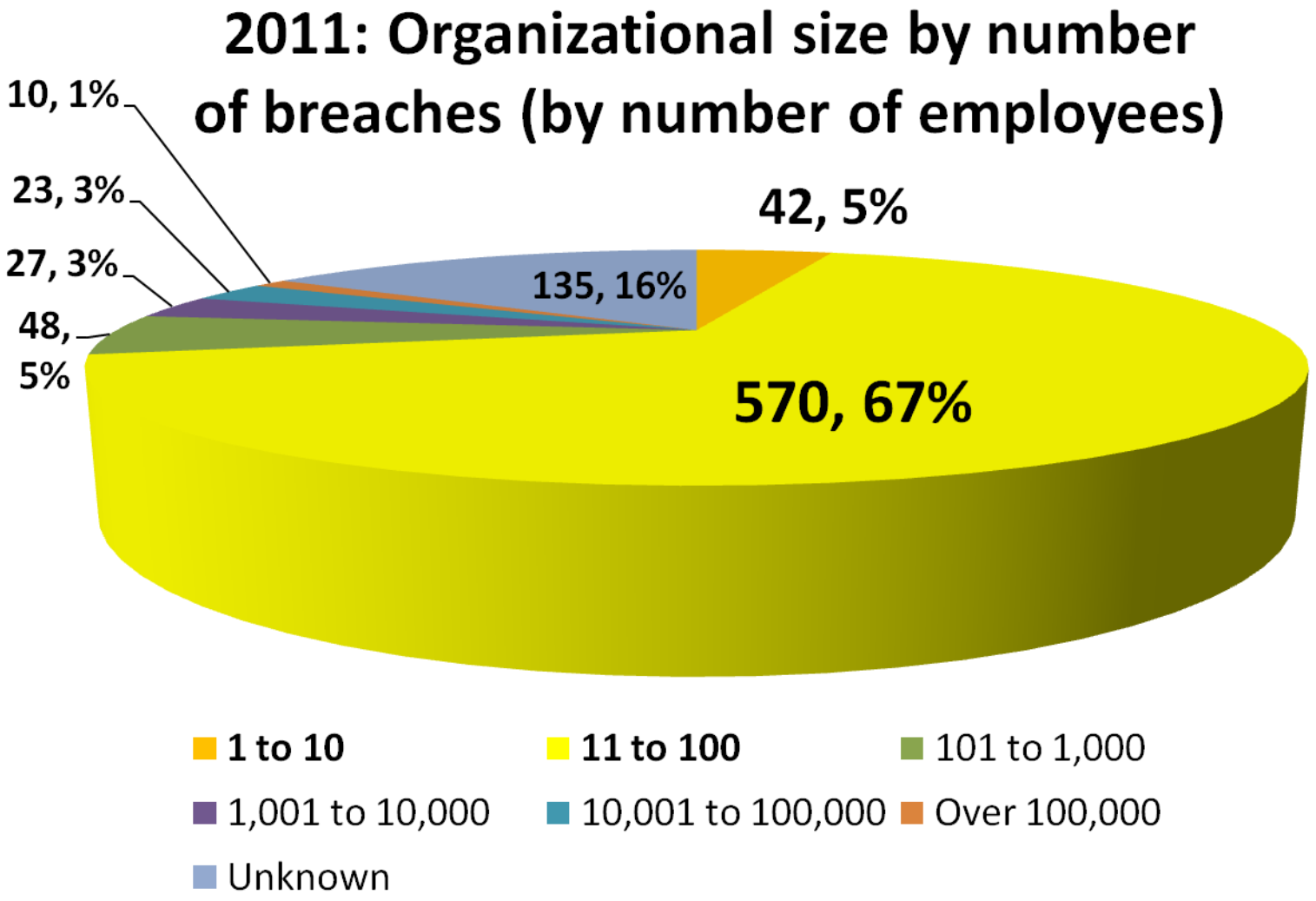
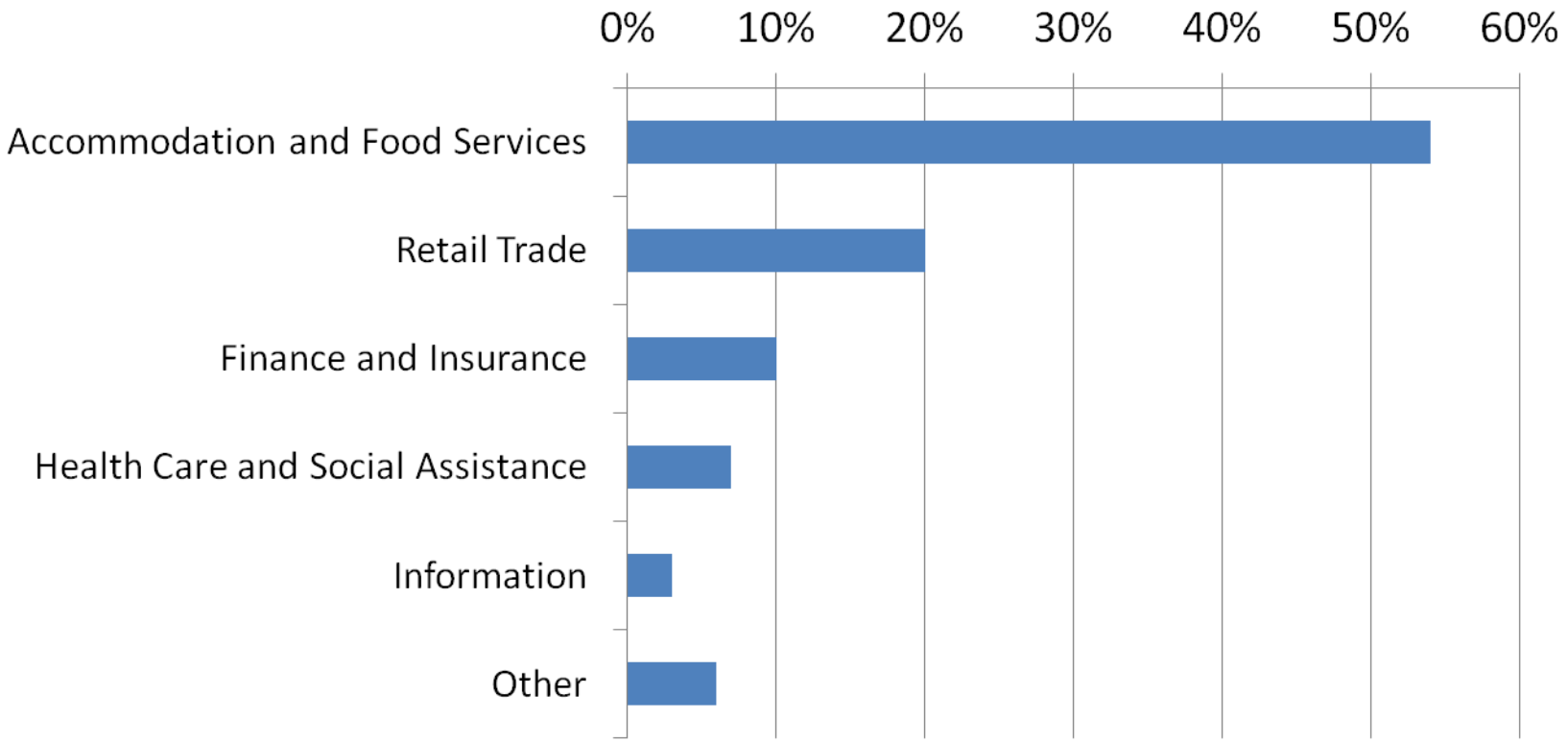
Cyber Safety for Small Businesses

Ryan Kriger
Assistant Attorney General, Public Protection Division
June 20, 2012



Source: 2012 Verizon Data Breach Investigations Report
(855 incidents in dataset)

2011: Industry Groups Represented by Percent of Breaches



Source: 2012 Verizon Data Breach Investigations Report
(855 incidents in dataset)

2011 DATA BREACHES

WHO IS BEHIND DATA BREACHES?	
98%	stemmed from external agents (+6%)
4%	implicated internal employees (-13%)
<1%	committed by business partners (<>)
58%	of all data theft tied to activist groups

Source: 2012 Verizon Data Breach Investigations Report
(855 incidents in dataset)

2011 DATA BREACHES

HOW DO BREACHES OCCUR?	
81%	utilized some form of hacking (+31%)
69%	incorporated malware (+20%)
10%	involved physical attacks (-19%)
7%	employed social tactics (-4%)
5%	resulted from privilege misuse (-12%)

Source: 2012 Verizon Data Breach Investigations Report
(855 incidents in dataset)

2011 DATA BREACHES

WHAT COMMONALITIES EXIST?	
79%	of victims were targets of opportunity (-4%)
96%	of attacks were not highly difficult (+4%)
94%	of all data compromised involved servers (+18%)
85%	of breaches took weeks or more to discover (+6%)
92%	of incidents were discovered by a third party (+6%)
97%	of breaches were avoidable through simple or intermediate controls (+1%)
96%	of victims subject to PCI DSS had not achieved compliance (+7%)

Source: 2012 Verizon Data Breach Investigations Report (855 incidents in dataset)

Vermont's Security Breach Notice Act

- 9 V.S.A. § 2430 and § 2435
- Applies to Businesses and State Agencies
  - Enforced by either AG or DFR (was BISHCA)
  - Does Not Apply to Certain Financial Institutions
- Amended Effective May 8, 2012

Definition of “Security Breach”

“unauthorized acquisition of electronic data or a reasonable belief of an unauthorized acquisition of electronic data that compromises the security, confidentiality, or integrity of a consumer’s **personally identifiable information** maintained by the data collector.”

Definition of “Security Breach”

“does not include **good faith** but unauthorized acquisition of personally identifiable information by an employee or agent of the data collector for a **legitimate purpose of the data collector**, provided that the personally identifiable information is **not used for a purpose unrelated to the data collector’s business** or subject to further unauthorized disclosure.”

Definition of “Security Breach”

Factors to consider when determining if a breach has occurred:

(i) Information is in someone else’s physical custody (*i.e.* stolen laptop);

(ii) Information has been downloaded or copied (*i.e.* hacking);

(iii) Information has been used by an unauthorized person (*i.e.* reports of fraudulent accounts opened or ID Theft); or

(iv) that the information has been made public.

What is Personally Identifiable Information (PII)?

First Name or First Initial & Last Name (if it has not been encrypted or rendered unreadable), AND

- Social Security number; OR
- Motor vehicle operator's license number or non-driver identification card number; OR
- Financial account number or credit or debit card number, if circumstances exist in which the number could be used without additional identifying information, access codes, or passwords; OR
- Account passwords or personal identification numbers or other access codes for a financial account.

I’ve Had a Data Breach, What Next?

1. Secure Your Data
2. Contact Law Enforcement
3. Contact Entities From Which You Obtained the Data
4. Notify the Attorney General’s Office Of The Breach
5. Notify Consumers Of The Breach
6. Notify the Credit Reporting Agencies (if more than 1,000 consumers)

Contact Law Enforcement

1. Call the FBI
2. Inform Them Of Your Duty To Notify Customers
3. Determine Whether Law Enforcement Wants You To Delay Notification

Timing of Notice Requirements

1. All Notices Should Go Out In The Most Expedient Time Possible
2. 14 Day Preliminary Notice to AG (non-public)
3. Final Notice to AG and to Customers (public) within 45 days
4. May only be delayed on request from law enforcement

Contents of Notice Requirements

- Incident in general terms.
- Type of PII accessed
- General acts taken to protect the PII from further breaches
- Telephone number, toll-free if available, for further information.
- Advice that directs the consumer to remain vigilant by reviewing account statements and monitoring free credit reports.
- The approximate date of the security breach.

Manner of Notice Requirements

- Direct Notice
  - Mail
  - Email (if requirements are met)
  - Telephone (not prerecorded)
- Substitute Notice (Website and Major Media)
  - If cost would exceed $5,000
  - If number of customers exceeds 5,000
  - If insufficient contact information

No Harm Letter

- Notice Not Required if Misuse of Personal Information is Not Reasonably Possible
- Notice of this determination with detailed explanation sent to Vermont Attorney General

Penalty for Noncompliance

- Violation of the Consumer Protection Act
- $10,000 Civil Penalty per Violation
- Violation = Customer Not Noticed Per Day

Social Security Number Protection Act

- 9 V.S.A. §§ 2440, 2445
- Applies to businesses and state agencies
- Businesses must safely destroy records that Contain Social Security Numbers and other personal information

Social Security Number Protection Act

A business may not:

- Make SSN's Public
- Put a SSN on a membership card
- Require non-secure or non-encrypted internet transmission of SSN's
- Require SSN to logon to website, unless with password or PIN
- Print SSN on mailings (unless required by law)
- Disclose SSNs to 3rd Parties without Written Consent

Social Security Number Protection Act

Exceptions:

- SSN mailed in application or account documents, but not on a postcard or on the envelope
- Use of SSN “reasonably necessary for administrative purposes or internal verification”
- Opening of account or the provision of or payment for a product or service authorized by an individual
- Acting pursuant to a court order, subpoena, otherwise required by law
- Providing SSNs to government entity, including law enforcement
- Redacted SSN
- Info obtained from official records or court records
- Use by business prior to 1/1/2007

Social Security Number Protection Act

Exceptions – Use of SSN to:

- investigate or prevent fraud
- conduct background checks
- conduct social or scientific research
- collect a debt
- obtain a credit report from or furnish data to a consumer reporting agency pursuant to the fair credit reporting act
- undertake a permissible purpose enumerated under Gramm Leach Bliley
- locate an individual who is missing, is a lost relative, or is due a benefit, such as a pension, insurance, or unclaimed property benefit.

Unfair and Deceptive Acts Statutes

- Vermont's Consumer Protection Act
- The FTC Act
- Prohibits Unfair and Deceptive Acts
- Unfair: Collecting Sensitive Information and Failing to Properly Protect It
- Deceptive: Advertising That You Protect Information When You Do Not

HIPAA

- Health Insurance Portability and Accountability Act
- Applies to Health Plans, Health Care Providers and Health Care Clearinghouses
- Protection of Personal Health Information
- Privacy Rule and Security Rule
- http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html

COPPA

- Children's Online Privacy Protection Act
- Applies to Website Operators that collect personal information from children under 13
- Requires Privacy Notice & Verifiable Parental Consent for Collection, Use andDisclosure of Personal Information
- Privacy Rule and Security Rule
- http://www.coppa.org

Gramm-Leach-Bliley Act

- Applies to Financial Institutions (companies that offer consumers financial products or services like loans, financial or investment advice, or insurance)
- Requires Companies that offer financial services to give consumers privacy notices that explain their information-sharing practices
- http://business.ftc.gov/documents/bus53-brief-financial-privacy-requirements-gramm-leach-bliley-act

DFR (formerly BISHCA) Regs

- Regulation B-2001-01: Governs treatment of nonpublic personal info about consumers by financial institutions
- Regulation IH-2001-01: Governs treatment of nonpublic personal financial and health info about consumers by licensees under 8 V.S.A. Parts 3 & 4
- Regulation IH-2002-03: Standards for protecting security, confidentiality, and security of customer info under Gramm-Leach-Bliley

Online Resources

- VT Attorney General Site (http://www.atg.state.vt.us/issues/consumer-protection/privacy-and-Data-Security.php)
- OnGuardOnline.gov
- business.ftc.gov

Other Programs Coming Soon

- Cyber Safety for Small Businesses
- Scan Vermont
- Weekend Cyber Security Bootcamp
- Privacy and Data Security Round Table

Go to Privacy and Data Security at

www.atg.state.vt.us